# PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-027231
(43)Date of publication of application : 25.01.2002

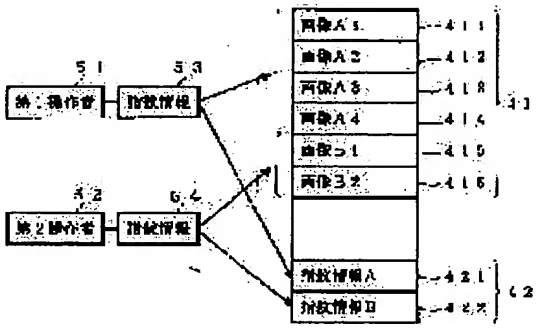
(51)Int.CI. H04N 1/387
G06F 12/14
G06T 1/00
G09C 5/00
H04L 9/08
H04L 9/32

(21)Application number : 2000-208383
(22)Date of filing : 10.07.2000

(71)Applicant : FUJITSU LTD
(72)Inventor : HIRANO HIDEYUKI

## (54) DATA I/O DEVICE

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a method of managing data which prevents infringement of copyright by distributing coded digital contents and prevents the destruction or missing of authorization data for decoding the coded digital contents.
SOLUTION: When storing image data A1-A4 of digital contents in a data region 41 of a recording medium, finger prints information 53 of an operator 51 used when coding the data or further coding a coding key is stored in a managed region 42 of the recording medium from or in which a general user cannot read or write data.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's

(54481 JP01)
先行技術

(19)日本国特許庁（JP）　(12)公開特許公報（A）　(11)特許出願公開番号
特開2002－27231
(P2002－27231A)
(43)公開日　平成14年1月25日(2002.1.25)

| (51)Int.Cl.' | 識別記号 | FI | | テーマコード'(参考) |
|---|---|---|---|---|
| H04N 1/387 | | H04N 1/387 | | 5B017 |
| G06F 12/14 | 320 | G06F 12/14 | 320B | 5B047 |
| | | | 320A | 5B057 |
| G06T 1/00 | 400 | G06T 1/00 | 400G | 5C076 |
| | 500 | | 500B | 5J104 |

審査請求　未請求　請求項の数10　OL　（全 11 頁）　最終頁に続く

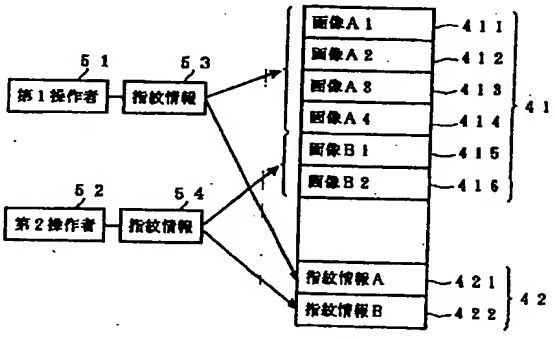
(21)出願番号　特願2000－208383(P2000－208383)
(22)出願日　平成12年7月10日(2000.7.10)

(71)出願人　000005223
富士通株式会社
神奈川県川崎市中原区上小田中４丁目１番１号
(72)発明者　平野　秀幸
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内
(74)代理人　100094145
弁理士　小野　由己男　（外２名）

最終頁に続く

(54)【発明の名称】　データ入出力装置

(57)【要約】
【課題】　デジタルコンテンツを暗号化して配布することで著作権の侵害を防止し、かつ暗号化されたデジタルコンテンツを復号化するための許諾情報が破壊されたり、紛失したりすることを防止するデータ運用方法を提供する。
【解決手段】　デジタルコンテンツである画像データＡ１～Ａ４を記録媒体中のデータ領域４１内に格納する際に、暗号化もしくは暗号鍵をさらに暗号化する際に用いた操作者５１の指紋情報５３を、一般利用者がリード・ライト不能な記録媒体の管理領域４２内に格納する。



1

【特許請求の範囲】

【請求項１】操作者の生体情報を読み取るための生体情報読取手段と、

配布するデジタルコンテンツを、不正に利用することが不可能となるように、前記生体情報読取手段によって読み取った生体情報に基づいて加工し、記録媒体に格納するデジタル情報記録手段と、

前記生体情報読取手段で読み取った生体情報を、前記記録媒体中の書き換え不能な領域に格納する生体情報記録手段と、を備えるデータ入出力装置。

【請求項２】前記生体情報読取手段によって読み取った生体情報と、前記記録媒体中の書き換え不能な領域に格納されている生体情報とを照合する生体情報比較手段と、

前記生体情報比較手段の照合結果に基づいて、前記記録媒体に格納されているデジタルコンテンツを利用可能状態に復元するデジタル情報復元手段と、をさらに備える、請求項１に記載のデータ入出力装置。

【請求項３】前記デジタル情報記録手段は、

前記デジタルコンテンツを暗号鍵によって暗号化して実データ部を作成するデータ暗号化手段と、

前記デジタルコンテンツの一部をサンプルデータとして抽出し、前記サンプルデータに前記暗号鍵に関する情報を含む許諾情報を電子透かしとして埋め込んだサンプルデータ部を作成するサンプルデータ作成手段と、

前記実データ部とサンプルデータ部とを合成した合成データ部を作成し、前記合成データを記録媒体に格納する合成データ作成手段と、を備える、請求項１または２に記載のデータ入出力装置。

【請求項４】前記デジタル情報復元手段は、

前記サンプルデータ部に埋め込まれた許諾情報を取り出して、前記暗号鍵を復元する暗号鍵復元手段と、

前記暗号鍵復元手段により復元された暗号鍵により、前記デジタルコンテンツ中の実データ部を復号化する復号化手段と、を備える、請求項３に記載のデータ入出力装置。

【請求項５】前記サンプルデータ部および復号化された実データ部を再生するデジタルデータ再生手段をさらに備える、請求項４に記載のデータ入出力装置。

【請求項６】前記デジタル情報記録手段は、

前記デジタルコンテンツ中に付加情報を配置してサンプルデータを作成するサンプルデータ作成手段と、

前記付加情報を配置する位置を含む前記デジタルコンテンツの一部を部分データ部として複製し、この部分データ部を暗号鍵によって暗号化して暗号化部分データ部を作成する部分データ作成手段と、

前記付加情報が前記デジタルコンテンツに配置される際の位置およびサイズに関するデータ合成情報と、前記暗号鍵の情報を含む許諾情報とを、前記デジタルコンテンツ中に電子透かしとして埋め込んで許諾情報付きデータ部を作成する許諾情報付きデータ部作成手段と、

前記暗号化部分データ部と許諾情報付きデータ部とを合成した合成データを作成し、これを記録媒体に格納する合成データ作成手段と、を備える、請求項１または２に記載のデータ入出力装置。

2

【請求項７】前記デジタル情報復元手段は、

前記許諾情報付きデータ部に埋め込まれたデータ合成情報および許諾情報を取り出して、前記許諾情報から前記暗号鍵を復元する暗号鍵復元手段と、

前記暗号鍵復元手段により復元された暗号鍵を用いて前記暗号化部分データ部を部分データ部として復号化し、復号化された部分データ部を前記データ合成情報に基づいて前記サンプルデータに合成して前記デジタルコンテンツを復元する復号化手段と、を備える、請求項６に記載のデータ入出力装置。

【請求項８】前記許諾情報は、前記生体情報読取手段によって読み取った生体情報によって前記暗号鍵を暗号化して生成する、請求項３～７のいずれかに記載のデータ入出力装置。

【請求項９】前記暗号鍵は前記生体情報読取手段によって読み取った生体情報に基づくデジタルデータである、請求項３～７のいずれかに記載のデータ入出力装置。

【請求項１０】前記生体情報は指紋情報である、請求項１～９のいずれかに記載のデータ入出力装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、データ入出力装置に関し、特に、暗号化されたデジタルコンテンツや付加情報が配置されたデジタルコンテンツを記録媒体に記録し、またはこれを再生するためのデータ入出力装置に関する。

【０００２】

【従来の技術】コンピュータプログラムなどのソフトウェアや電子出版物では、光磁気ディスク（ＭＯ）、ディジタルビデオディスク（ＤＶＤ）、フロッピー（登録商標）ディスク（ＦＤ）、ミニディスク（ＭＤ）、その他の記録媒体上に電子化データを格納して販売される。このような電子化データは、一般にコピーが容易であり、不正コピーが頻繁に行われている。このため、ソフトウェアベンダーや出版者側の著作権が侵害され著しく利益が阻害されるおそれがある。

【０００３】また、インターネットやＣＡＴＶ、その他のネットワークなどを通じて配布される静止画像データ、動画像データを含む電子化データについても同様にして不正コピーが頻繁に行われ、著作権者の利益が損なわれている。

【０００４】このような記録媒体上に格納された電子化データや各種ネットワークを通じて配布される電子化データなどのいわゆるデジタルコンテンツを保護するために、暗号鍵を用いてデジタルコンテンツを暗号化しこの

暗号化された実データを配布することが行われる。

【０００５】たとえば、ユーザが自分のパーソナルコンピュータからコンテンツの配布者側にアクセスを行い、デジタルコンテンツをハードディスク上にダウンロードを行ってこれを利用する場合を考える。まず、ユーザはホストコンピュータにアクセスしてダウンロードのためのプラグインモジュールを入手する。この後、使用しているハードディスクドライブの識別番号、使用しているコンピュータのＣＰＵ識別番号、その他ユーザ固有の識別情報をホストコンピュータ側に送付する。

【０００６】コンテンツの配布者側では、デジタルコンテンツをコンテンツ鍵で暗号化した実データと、コンテンツ鍵をユーザ固有の識別情報で暗号化した許諾情報を、ユーザ側に送信する。

【０００７】ユーザ側では、送られてきた暗号化実データと、許諾情報とを暗号化された状態のままハードディスクに記録する。デジタルコンテンツを利用する場合には、ハードディスクドライブの識別番号などのユーザ固有の識別情報を用いて、許諾情報を復号化し、コンテンツ鍵を取得する。このコンテンツ鍵を用いて、暗号化されたデジタルコンテンツを復号化してこれを利用する。

【０００８】この場合、ユーザ個々にデジタルコンテンツの利用権を与える際に、デジタルコンテンツを暗号化するための暗号鍵を共通にすることができ、ユーザ毎に異なるユーザ固有の情報を用いて復号鍵を暗号化することによって、利用権を個々に与えることが可能となる。

【０００９】上述の方法でデータの配布を行う場合、データ配布者は暗号化されたデジタルコンテンツと、暗号化されたデジタルコンテンツの復号鍵となる許諾情報とを別々に送付する必要がある。

【００１０】また、ユーザ側においても、送付されてくる暗号化されたデジタルコンテンツとその許諾情報とを別々に記録媒体に格納しておく必要がある。したがって、データ配布者側からユーザ側に送付される途中で許諾情報が破壊されたり、またはユーザ側の記録媒体上で許諾情報がなんらかの事故により破壊もしくは紛失した場合には、デジタルコンテンツを利用することができなくなり、再度許諾情報を入手する手順が必要となる。

【００１１】また、図書館の写本、美術館所蔵品などを写真やスキャナなどで画像データとして取り込み、これをユーザに利用させる場合、画像データが完全に暗号化されていると許諾情報のやりとりを行う前に、ユーザ側で所望の画像データを特定することが困難である。したがって、画像の一部がユーザ側で確認でき、かつ不正に流用されることがないように運用することが望ましい。

【００１２】このために、特開平8-241403号公報に示されるような、デジタルコンテンツに著作権情報などの付加情報を可視的な電子透かしとして埋め込んで配布することが考えられる。

【００１３】デジタルコンテンツに可視的な電子透かしとして付加情報を埋め込んで配布する場合、この付加情報を除去して元のデジタルコンテンツを復元するために、色度または輝度の変調データを画素毎に作成し、これを付加情報付きデジタルコンテンツと一緒に配布する必要があり、このようなデータの送受信に時間を要するとともに、データを格納するためのメモリ容量が大きく取られるという問題がある。

【００１４】上述したような静止画像や動画像を含む画像データばかりでなく、音楽データや音声データ、地図データなどの各種デジタルデータについても同様の問題点を内包している。

【００１５】

【発明が解決しようとする課題】本発明は、デジタルコンテンツの著作権や版権を損なうことなく、正規のユーザによる利用を容易にするデータ入出力装置を提供する。

【００１６】

【課題を解決するための手段】本発明に係るデータ入出力装置は、操作者の生体情報を読み取るための生体情報読取手段と、配布するデジタルコンテンツを、不正に利用することが不可能となるように、生体情報読取手段によって読み取った生体情報に基づいて加工し、記録媒体に格納するデジタル情報記録手段と、生体情報読取手段で読み取った生体情報を、記録媒体中の書き換え不能な領域に格納する生体情報記録手段とを備える。

【００１７】ここで、生体情報読取手段によって読み取った生体情報と記録媒体中の書き換え不能な領域に格納されている生体情報とを照合する生体情報比較手段と、生体情報比較手段の照合結果に基づいて、記録媒体に格納されているデジタルコンテンツを利用可能状態に復元するデジタル情報復元手段とをさらに備える構成とすることが可能である。

【００１８】また、デジタル情報記録手段は、デジタルコンテンツを暗号鍵によって暗号化して実データ部を作成するデータ暗号化手段と、デジタルコンテンツの一部をサンプルデータとして抽出し、サンプルデータに前記暗号鍵に関する情報を含む許諾情報を電子透かしとして埋め込んだサンプルデータ部を作成するサンプルデータ作成手段と、実データ部とサンプルデータ部とを合成した合成データ部を作成し、合成データを記録媒体に格納する合成データ作成手段とを備える構成とすることができる。

【００１９】さらに、デジタル情報復元手段は、サンプルデータ部に埋め込まれた許諾情報を取り出して、暗号鍵を復元する暗号鍵復元手段と、暗号鍵復元手段により復元された暗号鍵により、デジタルコンテンツ中の実データ部を復号化する復号化手段とを備える構成とすることができる。

【００２０】ここで、サンプルデータ部および復号化された実データ部を再生するデジタルデータ再生手段をさ

らに備える構成とすることができる。また、デジタル情報記録手段は、デジタルコンテンツ中に付加情報を配置してサンプルデータを作成するサンプルデータ作成手段と、付加情報を配置する位置を含むデジタルコンテンツの一部を部分データ部として複製し、この部分データ部を暗号鍵によって暗号化して暗号化部分データ部を作成する部分データ作成手段と、付加情報がデジタルコンテンツに配置される際の位置およびサイズに関するデータ合成情報と暗号鍵の情報を含む許諾情報とをデジタルコンテンツ中に電子透かしとして埋め込んで許諾情報付きデータ部を作成する許諾情報付きデータ部作成手段と、暗号化部分データ部と許諾情報付きデータ部とを合成した合成データを作成し、これを記録媒体に格納する合成データ作成手段とを備える構成とすることが可能である。

【００２１】さらに、デジタル情報復元手段は、許諾情報付きデータ部に埋め込まれたデータ合成情報および許諾情報を取り出して、許諾情報から暗号鍵を復元する暗号鍵復元手段と、暗号鍵復元手段により復元された暗号鍵を用いて暗号化部分データ部を部分データ部として復号化し、復号化された部分データ部をデータ合成情報に基づいてサンプルデータに合成してデジタルコンテンツを復元する復号化手段とを備える構成とすることができる。

【００２２】また、許諾情報は生体情報読取手段によって読み取った生体情報によって暗号鍵を暗号化して生成するように構成でき、暗号鍵を、生体情報読取手段によって読み取った生体情報に基づくデジタルデータとすることも可能である。

【００２３】この生体情報は操作者の指紋情報とすることが可能であり、操作者の網膜情報、虹彩情報、声紋に関する情報などを用いることも可能である。

【００２４】

【発明の実施の形態】◎第１実施形態

〔概略構成〕図１は、本発明に係るデータ入出力装置の１実施形態の概要構成を示す制御ブロック図である。

【００２５】データ入出力装置１は、配布を行うデジタルコンテンツを入力するための映像や音などのデータ入力手段１１、操作者の生体情報を読み取るための生体情報読取手段１２、入力されるデジタルコンテンツを生体情報読取手段１２により読み取った生体情報に基づいて処理を行うデータ処理部１３、データ処理部１３で処理されたデジタルコンテンツを記録媒体１７に記録するための記録部１４、記録媒体１７に格納されているデータを読み出すためのデータ読取部１５、データを再生するための再生手段１６などを備えている。

【００２６】ここで、生体情報読取手段１２は、操作者の指紋情報を読み取るための指紋読取装置で構成することができ、生体情報として網膜情報、虹彩情報、声紋情報などを用いる場合には、それぞれ網膜情報、虹彩情報、声紋情報を読み取る情報読取装置のうちのいずれか１つまたはこれらの組み合わせで構成することも可能である。

【００２７】また、記録媒体１７は、光磁気ディスク（ＭＯ）、フロッピーディスク（ＦＤ）、ＤＶＤＲＡＭ、ＤＶＤＲＷ、ＣＤ－Ｒ、ＣＤ－ＲＷ、ＩＣカード、フラッシュメモリ、ＤＡＴ、ＶＴＲなどの各種記録媒体を利用することが可能であり、記録部１４およびデータ読取部１５は、使用する記録媒体に応じた書き込みヘッドおよび読取ヘッドで構成できる。

【００２８】配布を行うデジタルコンテンツは、静止画像や動画像をなどの画像データ、音楽や音声などの音データ、画像データと音データとを複合的に含むデータなどで構成することができ、再生手段１６は配布を行うデジタルコンテンツに応じて、液晶ディスプレイやＣＲＴなどの画像表示手段、スピーカなどの音声表示手段およびこれらの組み合わせで構成することが可能である。この再生手段１６は、データ入出力装置１に内蔵させることも可能であり、外部装置として接続する形態をとることも可能である。

【００２９】〔データ処理部〕データ処理部１３を図２に基づいて説明する。データ処理部１３は、コンテンツ鍵生成部２１、コンテンツ暗号化部２２、生体情報処理部２３、コンテンツ鍵暗号化部２４、サンプルデータ生成部２５、許諾情報入サンプル作成部２６、暗号化コンテンツ合成部２７などを備えている。

【００３０】コンテンツ鍵生成部２１は、データ入力手段から入力されるデジタルコンテンツを暗号化するためのコンテンツ鍵を生成するものであり、たとえば、コンテンツ鍵となる乱数を生成する乱数発生器の構成とすることができる。また、データ読取部１５によって読み取った記録媒体１７の媒体ＩＤをコンテンツ鍵生成部２１により管理し、デジタルデータを暗号化する際のコンテンツ鍵として用いるように構成することもできる。

【００３１】コンテンツ暗号化部２２は、コンテンツ鍵生成部２１によって生成されたコンテンツ鍵を用いてデジタルコンテンツを暗号化する。生体情報処理部２３は、生体情報読取手段１２によって読み取った生体情報をHASH関数などを用いて圧縮し、暗号鍵の暗号化に用いることが可能となるようにデジタル処理を行う。

【００３２】コンテンツ鍵暗号化部２４は、生体情報処理２３でデジタル処理された生体情報を用いてコンテンツ鍵の暗号化を行う。サンプルデータ生成部２５では、デジタルコンテンツの一部を部分データ部として抽出する。

【００３３】許諾情報入サンプル作成部２６は、サンプルデータ生成部２５で抽出した部分データ部に、生体情報および生体情報で暗号化した暗号鍵の情報を含む許諾情報を不可視の電子透かしとして埋め込んで、許諾情報入サンプルデータ部を作成する。このとき、電子透かし

は、デジタルコンテンツの特定の周波数帯域に挿入するように構成でき、または、データの一部を間引きしてここに挿入するように構成することもできる。

【００３４】暗号化コンテンツ合成部２７は、許諾情報入サンプルデータ部と暗号鍵によって暗号化されたデジタルコンテンツを合成して合成データ部を作成する。また、データ処理部１３は、サンプルデータ表示部３１、許諾情報抽出部３２、生体情報照合部３３、コンテンツ鍵復号部３４、コンテンツ復号部３５、コンテンツ動作部３６などを備えている。

【００３５】サンプルデータ表示部３１は、データ読取部１５によって読み取った合成データのうちサンプルデータ部を再生手段１６により再生させる。許諾情報抽出部３２は、合成データのサンプルデータ部に埋め込まれた許諾情報を抽出する。

【００３６】生体情報照合部３３は、抽出された許諾情報中の生体情報と、新たに生体情報読取手段１２によって読み取った生体情報とを照合し、一致するか否かを判別する。

【００３７】コンテンツ鍵復号部３４は、生体情報を用いて、サンプルデータ部から抽出した許諾情報中の暗号鍵を復号化する。コンテンツ復号部３５は、復号化した暗号鍵を用いてデジタルデータの復号化を行う。

【００３８】コンテンツ動作部３６は、復号化したデジタルデータを再生手段１６により再生させる。

〔動作の概略〕生体情報として指紋情報を利用する場合について、その動作を図３に示すフローチャートに基づいて説明する。

【００３９】電源が投入されると、ステップＳ１において各パラメータを初期化するなどして初期設定を行う。ステップＳ２では、指紋登録モードが指示されたか否かを判別する。データ入出力装置１に設けられた入力スイッチ（図示せず）を介して指紋登録モードが指示されたと判断した場合にはステップＳ３に移行する。

【００４０】ステップＳ３では、記録媒体１７に対して操作者の指紋情報の登録処理を実行する。たとえば、生体情報読取手段１２を介して操作者の指紋に関する画像データを読み取り、特徴点に関するデジタルデータを作成し、HASH関数により圧縮した指紋情報として記録媒体１７の管理領域に格納する。記録媒体１７は、図７、図８に示すように、一般利用者により利用可能なデータ領域４１と、一般利用者がリード・ライトすることが不可能な管理領域４２を備えており、この管理領域４２に指紋情報を書き込むように構成する。

【００４１】このとき、図７に示すように、ユーザ毎に指紋情報を格納するように構成することが可能である。この場合、たとえば第１操作者５１の指紋情報５３を管理領域４２の第１指紋情報領域４２１に格納し、第２操作者５２の指紋情報５４を管理領域４２の第２指紋情報領域４２２に格納するように構成できる。また、図８に示すように、単一のユーザでも異なる指の指紋情報を個別に格納するように構成することも可能である。この場合、たとえば、操作者５１の小指の指紋情報５５を管理領域４２の第１指紋情報領域４２１に格納し、中指の指紋情報５６を管理領域４２の第２指紋情報領域４２２に格納し、親指の指紋情報５７を管理領域４２の第３指紋情報領域４２３に格納するように構成することができる。

【００４２】ステップＳ４では、記録モードが選択されたか否かを判別する。データ入出力装置１の入力スイッチなどにより、記録モードが指示されたと判断した場合には、ステップＳ５に移行する。ステップＳ５では、記録媒体１７に対するデジタルコンテンツの記録処理を実行する。

【００４３】〈記録処理〉記録媒体１７へのデジタルコンテンツの記録処理は、図４に示すようなフローチャートに基づいて実行される。

【００４４】ステップＳ１１では、指紋情報に基づく記録管理を行うか否かを判別する。記録管理を行う旨の指示があった場合には、ステップＳ１２に移行する。ステップＳ１２では、生体情報読取手段１２からの指紋情報の入力を受け付ける。ステップＳ１３では、記録媒体１７の管理領域４２に格納されている指紋情報を読み出す。ステップＳ１４では、生体情報読取手段１２で読み取った指紋情報と、記録媒体１７に格納されている指紋情報を照合し、一致するか否かを判別する。記録媒体１７の管理領域４２に格納されている指紋情報が複数ある場合には、各指紋情報についてそれぞれ照合を行い、一致する指紋情報があればステップＳ１５に移行する。

【００４５】ステップＳ１５では、デジタルコンテンツである画像データを入力する。ステップＳ１６では、画像データを暗号化するとともにサンプルデータを合成した合成画像を作成し、記録媒体１７に記録する。

【００４６】ステップＳ１４において、生体情報読取手段１２で読み取った指紋情報が、記録媒体１７の管理領域４２の各指紋情報と一致しないと判断した場合には、ステップＳ１７に移行する。ステップＳ１７では、指紋情報が一致しない旨のエラー表示を行い処理を終了する。

【００４７】ステップＳ１１において、記録管理を行わない旨の指示があった場合には、ステップＳ１８に移行する。ステップＳ１８では、デジタルコンテンツとなる画像データの入力を行う。ステップＳ１９では、画像データを暗号化せずにそのままの状態で記録媒体１７に記録する。

【００４８】〈記録管理によるデータ処理〉図４ステップＳ１６における画像記録処理の一例を図５のフローチャートに基づいて説明する。

【００４９】ステップＳ２１では、入力された画像データからサンプルデータを抽出する。たとえば、入力され

たデジタルコンテンツが複数の静止画像を含む場合には、そのうちの１つの画像データを代表するサンプルデータとして抽出する。

【００５０】ステップＳ２２では、デジタルコンテンツを暗号化するための暗号鍵をコンテンツ鍵生成部２１により生成する。ここで用いられるコンテンツ鍵は、ランダムに発生した暗号鍵を用いることもでき、記録媒体１７から取得した媒体ＩＤを用いることも可能である。また、生体情報読取手段１２によって読み取った指紋情報を暗号鍵として用いることも可能である。

【００５１】ステップＳ２３では、生成した暗号鍵を用いてデジタルコンテンツの暗号化を行う。ステップＳ２４では、デジタルコンテンツの暗号化を行った暗号鍵に関する情報をさらに暗号化し許諾情報を作成する。この許諾情報は、たとえば、暗号鍵を操作者のパスワードや指紋情報で暗号化して作成することができ、アクセス回数の制限を行う場合にはこの画像データに対するアクセス制限回数と実際のアクセス回数のカウント値とを含む情報とすることができる。

【００５２】ステップＳ２５では、許諾情報および指紋情報をサンプルデータに不可視情報として埋め込んで許諾情報入サンプルデータ部を作成する。ここでは、サンプルデータとして抽出した画像データの特定の周波数帯域に、許諾情報および指紋情報を挿入するように構成することができ、またデータの一部を間引きしてここに許諾情報および指紋情報を挿入するように構成することも可能である。

【００５３】ステップＳ２６では、許諾情報入サンプルデータ部と暗号化したデジタルコンテンツとを合成した合成データを生成する。サンプルデータ部は、JPEGなどの構造化データ形式にし、これに暗号化されたデジタルコンテンツを追加合成することで合成データを生成することが可能となる。

【００５４】ステップＳ２７では、記録媒体１７に合成データを記録する。図７に示すように、操作者毎に指紋情報の登録を行った記録媒体に対して、データの記録を行う場合には、第１操作者５１の指紋情報５３が不可視情報として埋め込まれた画像データＡ１が第１データ領域４１１に記録され、同様に画像データＡ２～Ａ４が第２データ領域４１２～第４データ領域４１４に記録される。また、第２操作者５２の指紋情報５４が不可視情報として埋め込まれた画像データＢ１～Ｂ２が、それぞれ第５データ領域４１５～第６データ領域４１６に格納される。また、図８に示すように、同一の操作者であっても格納するデジタルコンテンツ毎に異なる指の指紋情報を用いてデータの差別化を図ることも可能である。図示したものでは、小指の指紋情報５５を有する画像データＡ１～Ａ４を第１データ領域４１１～４１４に格納し、中指の指紋情報５６を有する画像データＢ１～Ｂ２をデータ領域４１５～４１６に格納し、親指の指紋情報５７を有する画像データＣ１～Ｃ４をデータ領域４１７～４２０に格納するようにしている。操作者の数、各操作者の指紋情報の数、格納する画像数などはこれに限定されないことは言うまでもない。

【００５５】〈再生処理〉図３ステップＳ７の再生処理では、図６に示すようなフローチャートに基づいて動作する。

【００５６】ステップＳ３１では、サンプルデータの再生を行うか否かを判別する。記録媒体１７に格納されている合成データ中のサンプルデータ部を表示する旨の指示を受け付けた場合にはステップＳ３２に移行する。ステップＳ３２では、指紋情報や許諾情報が不可視情報として埋め込まれたサンプルデータ部を、再生手段１６を介して再生させる。サンプルデータ部は、デジタルコンテンツから一部が抽出されたものであって、静止画像、動画像、音楽データ、およびこれらの複合化されたデジタルデータであり、液晶表示装置、ＣＲＴ、その他の表示装置やスピーカなどで構成される再生手段１６によって、その画像データの表示および音声の発音がなされる。

【００５７】ステップＳ３３では、デジタルコンテンツ（実データ）の再生を行う旨の指示があったか否かを判別する。デジタルコンテンツの再生を行う旨の指示を受けた場合には、ステップＳ３４に移行する。

【００５８】ステップＳ３４では、再生指示のあったデジタルコンテンツが許諾情報に基づいて管理されたデータであるか否かを判別する。再生指示のあったデジタルコンテンツが管理されたデータである場合にはステップＳ３５に移行する。

【００５９】ステップＳ３５では、生体情報読取手段１２からの指紋情報の入力を受け付ける。ステップＳ３６では、再生指示のあったデジタルコンテンツのサンプルデータ部に埋め込まれた指紋情報を読み出す。ステップＳ３７では、生体情報読取手段１２で読み取った指紋情報と、デジタルコンテンツのサンプルデータ部から読み出した指紋情報を照合し、一致するか否かを判別する。各指紋情報が一致する場合にはステップＳ３８に移行する。

【００６０】ステップＳ３８では、記録媒体１７に格納されているデジタルコンテンツのサンプルデータ部に埋め込まれている許諾情報から暗号鍵を取り出す。ここでは、不可視情報としてサンプルデータ部に埋め込まれている許諾情報を抽出し、ステップＳ３６で読み出した指紋情報を用いて復号化を行うことで暗号鍵を取り出すことができる。

【００６１】ステップＳ３９では、復号化した暗号鍵を用いてデジタルコンテンツを復号化する。ステップＳ４０では、デジタルコンテンツの再生処理を行う。デジタルコンテンツは、静止画像、動画像、音楽データ、およびこれらの複合化されたデジタルデータで構成されてお

り、液晶表示装置、ＣＲＴ、その他の表示装置やスピーカなどで構成される再生手段１６によって、その画像データの表示および音声の発音がなされることにより再生される。

【００６２】ステップＳ３７において、生体情報読取手段１２で読み取った指紋情報と、サンプルデータ部に埋め込まれている指紋情報とが一致しないと判断した場合には、ステップＳ４１に移行する。ステップＳ４１では、指紋が一致しなかった旨の表示を行うなどのエラー処理を行い、この処理を終了する。

【００６３】〔第１実施形態の作用・効果〕この第１実施形態では、デジタルコンテンツからサンプルデータを抽出し、デジタルコンテンツを暗号化する際に用いた暗号鍵を指紋情報でさらに暗号化して不可視情報としてサンプルデータに埋め込んでいるので、許諾情報を持たない者が不正に記録媒体を入手しても利用することが不可能であり、高いセキュリティを維持することができる。また、サンプルデータ内に暗号鍵が埋め込んであるので、正当な利用者が暗号鍵を容易に取り出すことができ、暗号鍵の紛失などの問題がなくなる。また、指紋情報を一般利用者がリード、ライト不能な記録媒体の管理領域４２に格納しているので、さらに高いセキュリティを維持できる。

【００６４】〔第１実施形態の変形〕

（Ａ）デジタルコンテンツを暗号化する際の暗号鍵を、HASH関数により処理した指紋情報をそのまま用いる構成とすることができる。この場合、サンプルデータ部に不可視情報として埋め込まれる許諾情報は指紋情報と共通のものとすることができる。

【００６５】再生時には、許諾情報を読み出すことによって指紋情報を得ることができ、この指紋情報を用いてデジタルコンテンツの復号化を行うように構成できる。

（Ｂ）生体情報は、網膜の画像情報に基づく網膜情報や虹彩の画像情報に基づく画像情報、あるいは声紋情報などを用いることが可能である。

（Ｃ）図２において、コンテンツ鍵生成部２１～暗号化コンテンツ合成部２７からなる記録部２を含まないデータ再生装置を構成することが可能である。同様に、サンプルデータ表示部３１～コンテンツ動作部３６からなる再生部３を含まないデータ記録装置を構成することも可能である。

◎第２実施形態

〔概略構成〕第２実施形態では、第１実施形態と同様に、図１で示すような制御ブロック図でなる装置を想定できる。

【００６６】〔データ処理部〕この実施形態におけるデータ処理部１３を図９に基づいて説明する。データ処理部１３は、暗号鍵生成部６１、付加情報入力部６２、指紋情報処理部６３、画像加工部６４、画像暗号化部６５、許諾情報作成部６６，情報埋め込み部６７を備えている。

【００６７】暗号鍵生成部６１は、データ入力手段から入力されるデジタルコンテンツの一部を暗号化するための暗号鍵を生成するものであり、第１実施形態のコンテンツ鍵生成部２１と同様の構成とすることができる。

【００６８】付加情報入力部６２は、著作権情報などの付加情報入力および付加情報の埋め込み位置などを決定するためのものである。指紋情報処理部６３は、生体情報読取手段１２によって読み取った指紋情報をHASH関数などを用いて圧縮し、暗号鍵の暗号化に用いることが可能となるようにデジタル処理を行うものである。

【００６９】画像加工部６４は、デジタルコンテンツの一部を複製したり、原画像に付加情報を可視的に埋め込む機能を有するものである。画像暗号化部６５は、デジタルコンテンツから複製される部分データ部を暗号鍵で暗号化するものである。

【００７０】許諾情報作成部６６は、暗号鍵に関する情報および部分データ部の位置とサイズを示す画像合成情報を暗号化して許諾情報を作成するものである。情報埋め込み部６７は、暗号鍵に関する情報および画像合成情報を不可視情報としてデジタルコンテンツに埋め込むものである。

【００７１】また、データ処理部１３は、サンプルデータ表示部７１、許諾情報抽出部７２、指紋情報照合部７３、暗号鍵取出部７４、画像復号化部７５、コンテンツ動作部７６などを備えている。

【００７２】サンプルデータ表示部７１は、付加情報が可視的に追加されているデジタルコンテンツを再生手段１６により再生させる。許諾情報抽出部７２は、デジタルコンテンツ中に不可視情報として埋め込まれた許諾情報を抽出する。

【００７３】指紋情報照合手段７３は、記録媒体１７の管理領域に格納されている指紋情報と、生体情報読取手段１２から入力される指紋情報とを照合し一致するか否かを判別するものである。

【００７４】暗号鍵取出部７４は、デジタルコンテンツから取り出された許諾情報に基づいて暗号鍵を取り出すものである。画像復号化部７５は、取り出された暗号鍵を用いて暗号化された部分データ部を復号化して、合成情報に基づいてデジタルコンテンツを復元するものである。

【００７５】コンテンツ動作部７６は、復元されたデジタルコンテンツを動作させるものであり、静止画像や動画像の場合には液晶表示装置やＣＲＴなどの表示装置に表示を行い、音声データの場合にはスピーカなどに発音させるものである。

【００７６】〔記録処理〕この第２実施形態においても、第１実施形態と同様に、図３、図４に示したフローチャートのように動作する。ただし、図３ステップＳ５の記録処理については、図１０に示すフローチャートに

基づいて動作する。

【００７７】ステップＳ５１では、付加情報の入力を受け付ける。著作権者に関する情報や配布を行う管理者情報などのコンテンツ情報を、デジタルコンテンツ中に可視的な情報として埋め込む場合には、キーボードやその他入力手段からの入力を受け付けるか、あるいはデジタルコンテンツ中に含まれるコンテンツ情報を自動的に抽出することによって、付加情報の受付を行う。このとき、同時にデジタルコンテンツ中のどの位置に付加情報を追加するかの位置情報やサイズに関する画像合成情報を同時に取得する。

【００７８】ステップＳ５２では、暗号鍵生成部６１によって暗号鍵を生成する。この暗号鍵は、付加情報を追加する位置を含むデジタルコンテンツの一部を暗号化するためのものであり、生成した乱数に基づいて生成されたもの、記録媒体１７の媒体ＩＤに基づくもの、操作者のＩＤやパスワードに基づくものなどを想定することができる。

【００７９】ステップＳ５３では、画像合成情報に基づいて、この付加情報が追加される位置の部分データ部を複製する。ステップＳ５４では、複製された部分データ部を暗号鍵で暗号化する。

【００８０】ステップＳ５５では、デジタルコンテンツの原画像に、画像合成情報に基づく位置およびサイズで付加情報を可視的な情報として埋め込む。このとき、付加情報は、色度変調を伴う方法で可視的ウォーターマークとして埋め込むことが可能であり、また、輝度変調を伴う方法で埋め込むことも可能である。

【００８１】ステップＳ５６では、暗号鍵および画像合成情報を指紋情報で暗号化して許諾情報を作成する。この許諾情報は、暗号鍵および画像合成情報を記録媒体１７の媒体ＩＤで暗号化することも可能であり、また操作者のＩＤやパスワードによって暗号化することも可能であり、これらを適宜組み合わせて暗号化することも可能である。

【００８２】ステップＳ５７では、許諾情報および指紋情報をデジタルコンテンツ中に不可視情報として埋め込む。この場合、デジタルコンテンツの特定の周波数帯域に許諾情報および指紋情報を挿入するか、あるいはデータの一部を間引きしてここに許諾情報および指紋情報を挿入するように構成することが可能である。

【００８３】ステップＳ５８では、可視的な付加情報と不可視的な許諾情報および指紋情報を含むデジタルコンテンツと、暗号化された部分データ部とを合成して合成データを作成する。

【００８４】ステップＳ５９では、記録媒体１７のデータ領域に合成データを格納する。

〔再生処理〕この第２実施形態において記録媒体１７に格納されたデジタルコンテンツを再生する際には、第１実施形態の図６とほぼ同様の手順で処理することができる。

【００８５】ステップＳ３１では、付加情報が可視的に追加されたデジタルコンテンツ（サンプルデータ）の再生を行うか否かを判別する。サンプルデータを表示する旨の指示を受け付けた場合にはステップＳ３２に移行する。ステップＳ３２では、著作権者に関するの情報や配布を行う管理者情報などの付加情報が可視的に追加されたデジタルコンテンツの再生を行う。

【００８６】ステップＳ３３では、デジタルコンテンツ（実データ）の再生を行う旨の指示があったか否かを判別する。デジタルコンテンツの再生を行う旨の指示を受けた場合には、ステップＳ３４に移行する。

【００８７】ステップＳ３４では、再生指示のあったデジタルコンテンツが許諾情報に基づいて管理されたデータであるか否かを判別する。再生指示のあったデジタルコンテンツが管理されたデータである場合にはステップＳ３５に移行する。

【００８８】ステップＳ３５では、生体情報読取手段１２からの指紋情報の入力を受け付ける。ステップＳ３６では、再生指示のあったデジタルコンテンツのサンプルデータ部に埋め込まれた指紋情報を読み出す。ステップＳ３７では、生体情報読取手段１２で読み取った指紋情報と、デジタルコンテンツのサンプルデータ部から読み出した指紋情報を照合し、一致するか否かを判別する。各指紋情報が一致する場合にはステップＳ３８に移行する。

【００８９】ステップＳ３８では、記録媒体１７に格納されているデジタルコンテンツに不可視情報として埋め込まれている許諾情報から暗号鍵を取り出す。ここでは、不可視情報としてサンプルデータ部に埋め込まれている許諾情報を抽出し、ステップＳ３６で読み出した指紋情報を用いて復号化を行うことで暗号鍵を取り出すことができる。このとき、同時に付加情報が追加された位置とサイズを示す画像合成情報を復号化する。

【００９０】ステップＳ３９では、復号化した暗号鍵を用いて暗号化された部分データ部を復号化し、これをデジタルコンテンツに合成する。部分データ部は、付加情報が可視的に配置された位置を含む原画像の一部であり、画像合成情報に基づいて部分データ部をデジタルコンテンツ上に合成することで、元のデジタルコンテンツを復元することが可能となる。

【００９１】ステップＳ４０では、復元されたデジタルコンテンツの再生処理を行う。デジタルコンテンツは、静止画像、動画像、音楽データ、およびこれらの複合化されたデジタルデータで構成されており、液晶表示装置、ＣＲＴ、その他の表示装置やスピーカなどで構成される再生手段１６によって、その画像データの表示および音声の発音がなされることにより再生される。

【００９２】ステップＳ３７において、生体情報読取手段１２で読み取った指紋情報と、サンプルデータ部に埋

め込まれている指紋情報とが一致しないと判断した場合には、ステップＳ４１に移行する。ステップＳ４１では、指紋が一致しなかった旨の表示を行うなどのエラー処理を行い、この処理を終了する。

【００９３】〔第２実施形態の作用・効果〕この第２実施形態では、著作権者に関する情報や配布を行う管理者の情報に基づくコンテンツ情報を可視的な情報としてデジタルコンテンツ中に埋め込んでいるため、このままの状態で正常にデジタルコンテンツを利用することができない。また、この付加情報の位置やサイズに関する画像合成情報と、この位置における原画像を暗号化した暗号鍵の情報を含む許諾情報とを不可視情報としてデジタルコンテンツ中に含んでいるため、高いセキュリティを維持するとともに、正当な利用者が容易に復元して利用することが可能となる。また、暗号鍵の再発行などの無駄を省くことが可能となる。また、指紋情報を一般利用者がリード、ライト不能な記録媒体の管理領域に格納しているので、さらに高いセキュリティを維持できる。 ＊



＊【００９４】

【発明の効果】本発明によれば、操作者の生体情報に基づいて不正利用が不可能な状態にデジタルコンテンツを加工するとともに、記録媒体の書き換え不能領域にこの生体情報を格納しているため、高いセキュリティを維持できるとともに、暗号鍵の再発行の手間を省いて正当な利用者には容易に復元することが可能となる。

【図面の簡単な説明】

【図１】本発明の概略構成図。

【図２】データ処理部の構成図。

【図３】本発明の制御フローチャート。

【図４】本発明の制御フローチャート。

【図５】本発明の制御フローチャート。

【図６】本発明の制御フローチャート。

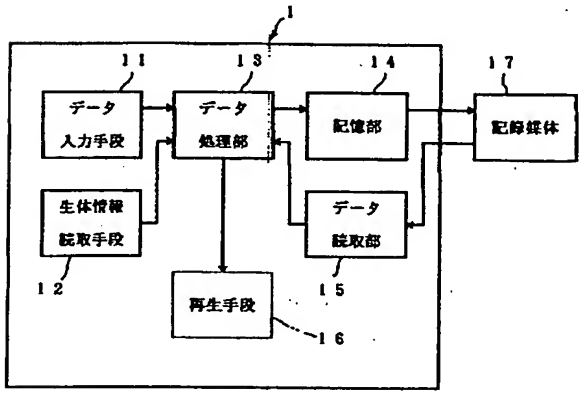
【図７】記録媒体へのデータ格納の概念説明図。

【図８】記録媒体へのデータ格納の概念説明図。

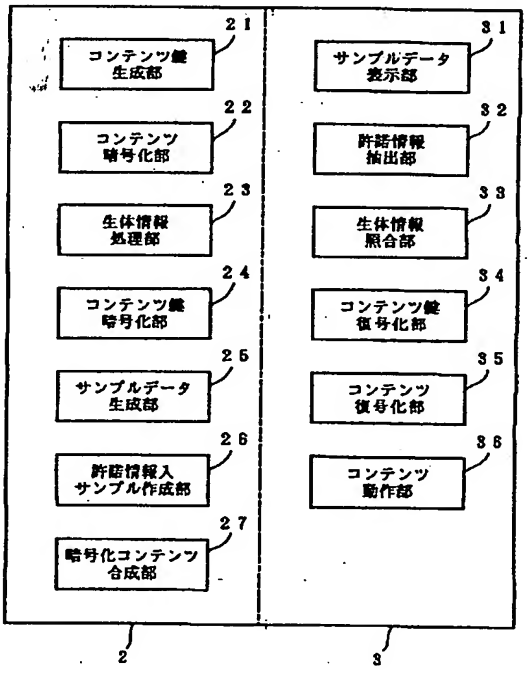
【図９】第２実施形態のデータ処理部の構成図。

【図１０】第２実施形態の制御フローチャート。

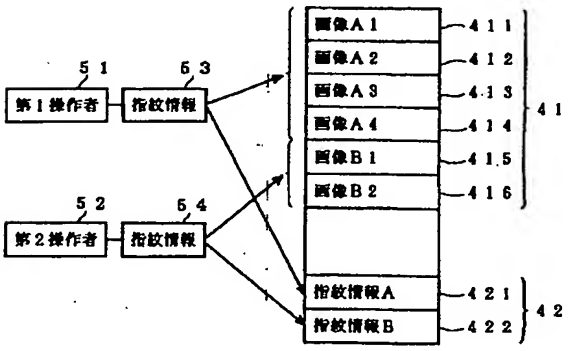
【図１】



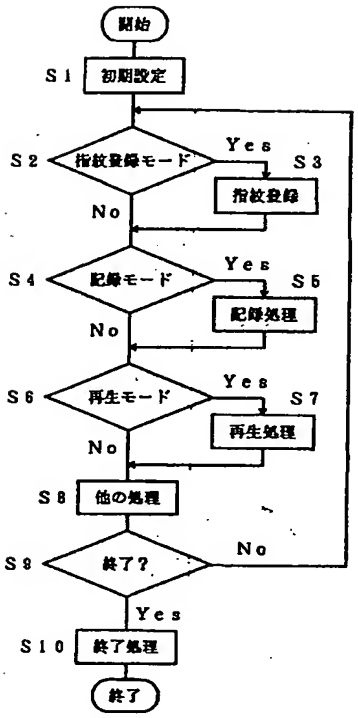

【図２】



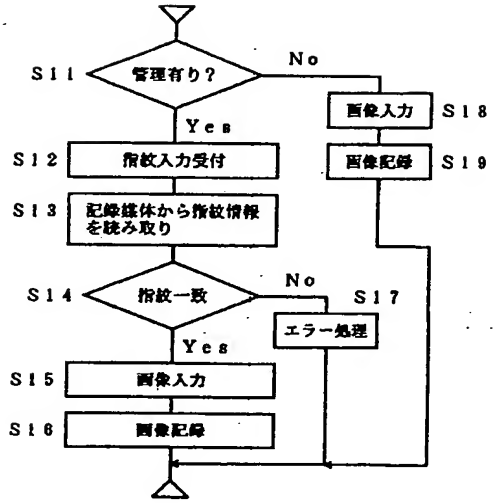

【図７】



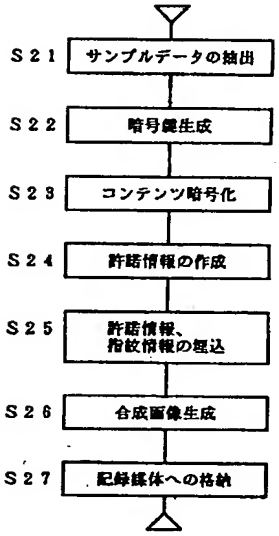
【図３】



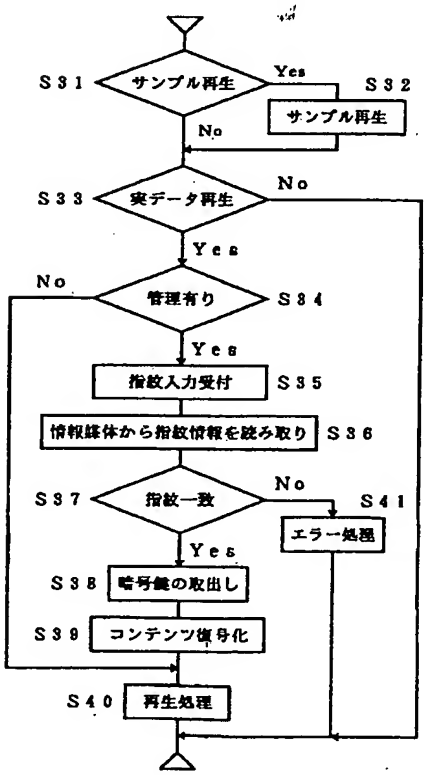

【図４】



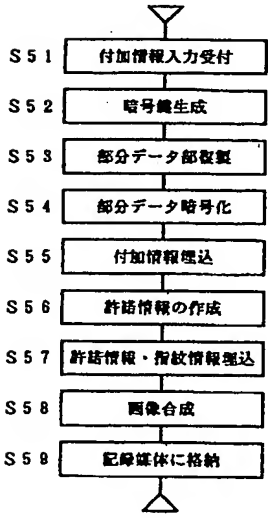

【図５】



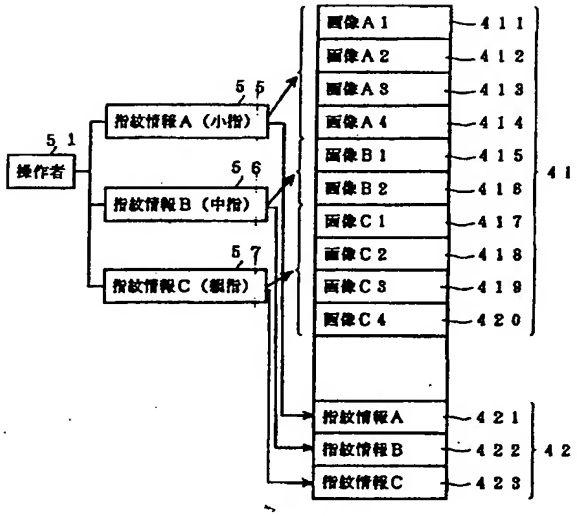

【図６】



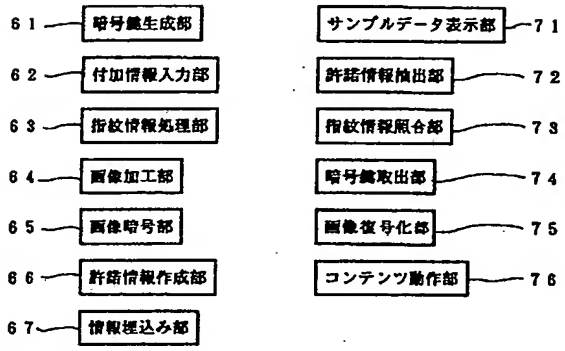

【図１０】



【図８】




【図９】




フロントページの続き

| (51)Int.Cl.' | 識別記号 | FI | | テーマコード (参考) |
|---|---|---|---|---|
| Ｇ０９Ｃ | 5/00 | Ｇ０９Ｃ | 5/00 | |
| Ｈ０４Ｌ | 9/08 | Ｈ０４Ｌ | 9/00 | ６０１Ｃ |
| | 9/32 | | | ６０１Ｅ |
| | | | | ６７３Ａ |
| | | | | ６７３Ｄ |

Ｆターム(参考) 5B017 AA03 BA05 BA07 CA08 CA09
5B047 AA25 BA02 CB25
5B057 CA12 CA16 CB12 CB16 CC01
CE08
5C076 AA14 BA06
5J104 AA14 EA04 EA17 EA25 EA26
KA01 KA16 KA17 NA02 NA12